

MANAGEMENT MEMO

NUMBER:

MM 02-07 (Revised)

SUBJECT:

DATE ISSUED:

FEBRUARY 22, 2002

FEBRUARY 27, 2002 (Revised)

EXPIRES:

WHEN RESCINDED

SECURITY AND RISK MANAGEMENT POLICY

REFERENCES:

STATE ADMINISTRATIVE MANUAL SECTION 4840

STATEWIDE INFORMATION MANAGEMENT MANUAL

GOVERNMENT CODE SECTIONS 11701 (b) & (g); 11710 (d) (i); 11712 (f)

BUDGET ACT OF 2001, 2001-02 FISCAL YEAR

ISSUING AGENCY:

DEPARTMENT OF INFORMATION
TECHNOLOGY

OVERVIEW:

This Management Memo revises the current SAM requirements for Security and Risk Management Policy for the State of California and adds information regarding future enhancements to the security policy and compliance requirements.

PURPOSE:

To establish and maintain a standard of due care to prevent misuse or loss of state agency information assets. This policy requires agencies to establish internal policies and adopt procedures that:

1. Establish and maintain management and staff accountability for protection of agency information assets;
2. Establish and maintain processes for the analysis of risks associated with agency information assets; and,
3. Establish and maintain cost-effective risk management processes intended to preserve agency ability to meet state program objectives in the event of the unavailability, loss or misuse of information assets.

POLICY:

State agencies need to ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction or disclosure and to ensure the physical security of these resources. State agency heads are accountable for the computerized information resources held by their agencies. They are responsible for the integrity of computerized information resources and the authorization of access to those resources. All agency employees share in this responsibility as well.

Agencies shall also ensure that users, contractors, and third parties having access to State computerized information resources are informed of and abide by this policy and the agency security plan and are informed of applicable state statutes related to computerized information resources.

Agency heads are responsible and shall take reasonable measures for implementation of, and compliance with, the state security policy. Each agency that employs information technology must establish risk

STATE ADMINISTRATIVE MANUAL

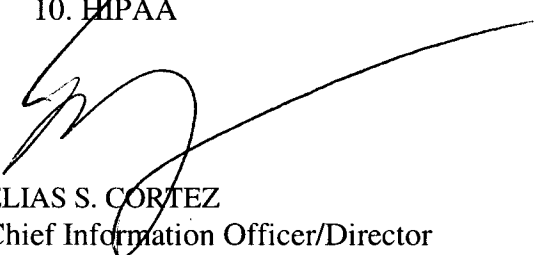
management and disaster recovery planning processes for identifying, assessing and responding to the risks associated with its information assets.

The state's information assets (its data processing capabilities, information technology infrastructure and data files) are an essential public resource. For many agencies, program operations would effectively cease in the absence of key computer systems. In some cases, public health and safety would be immediately jeopardized by the failure or disruption of a system. If state information systems and resources were to become unavailable it could have a detrimental impact on the state economy and the Californians who rely on state programs. Furthermore, the unauthorized modification, deletion or disclosure of information included in agency files and data bases can compromise the integrity of state programs, violate individual right to privacy and constitute a criminal act.

IMPLEMENTATION:

All state agencies must be in full compliance with existing security policies as stated in SAM (section 4840). In light of recent events, DOIT is undertaking activities to increase emphasis on compliance with security policies and to assist agencies in meeting their requirements. By 12/31/02, DOIT will build a statewide assessment methodology, which includes recommendations for evaluation in the following areas:

1. Security Management
2. Ethics, Law and Investigation
3. Security Architecture
4. Access Control
5. Physical & Environmental Security
6. Business Continuity
7. Computer Operations
8. Telecommunications and Network Security
9. Applications and Systems Development
10. HIPAA



ELIAS S. CORTEZ
Chief Information Officer/Director
State of California/Department of Information Technology